REMARKS

Applicants thank the Board of Patent Appeals and Interferences for considering Applicants' arguments. Applicants have amended independent Claims 21, 31, and 48 to more clearly define the claimed invention over the prior art. In particular, Applicants have amended independent Claims 21 and 48 to incorporate the subject matter of now canceled dependent Claims 27 and 49, respectively. Moreover, Applicants have amended independent Claim 31 to include similar subject matter.

Yet more, Applicants have amended each independent claim to also recite transposing an output of a final round from the plurality of transformation rounds. Support for this claim amendment is found at page 9, lines 16-27 of the present application. Applicants have also amended Claims 31-36 and 38 to address informalities.

Applicants submit that all claims are patentable, and present arguments and amendments herein supporting such patentability.

I. The Amended Claims

Independent Claim 21 is directed to a method of converting data between an unencrypted format and an encrypted format, the data being organized in bit words. The method includes converting the data by at least performing a plurality of transformation rounds, each transformation round having a respective round key and comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array. Each transformation round also includes exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that the at least one transformation is applied to the transposed state array, transposing the respective round key, and applying the respective transposed round key to the state array in at least one of the transformation rounds. The method also includes transposing an output of a final round from the plurality of transformation rounds.

Independent Claim 31 is a device counterpart to Claim 21. Independent claim 48 is similar to Claim 21, but further recites using 8-bit words, and operating on a state array comprising a 4x4 matrix of 8-bit words.

II. The Amended Claims Are Patentable

Ohkuma et al. discloses an apparatus for encrypting blocks of data. (Ohkuma et al.: Paragraphs 10-11). The encryption process occurs in multiple stages. (Paragraph 91-92). Ohkuma et al. also discloses that a matrix may be obtained by substituting rows, substituting columns, and arbitrarily transposing an arbitrary MDS matrix. (Paragraph 268). The Examiner correctly notes that Ohkuma et al. fails to disclose exchanging each of the rows with a respective column of the state array to form a transposed state array, as recited in independent Claims 21, 31, and 48. The Examiner looks to Luther to supply this deficiency.

Luther discloses an encryption system for two-dimensional data. The system of Luther encrypts through multiple encryption passes performed on binary data. In each pass, the mth row and the nth column of the binary data are encrypted. For each encryption pass, m and n are randomly selected and have a value, which is small relative to the size of the data. (Luther: Col. 1, lines 30-42).

Applicants have amended each of the independent claims to recite transposing the respective round key for each of the plurality of transformation rounds. Luther fails to disclose or fairly suggest such a feature. Differently, the transposition teachings of Luther relate to the process of confusing the already encrypted data and not to the claimed transposing of a round key. Furthermore, although Ohkuma et al. discloses transposing the MDS matrix, Ohkuma et al. fails to disclose or fairly suggest transposing the respective round key for each of the plurality of transformation rounds, as recited by each of the amended independent claims.

Moreover, Applicants submit that neither of these prior art references discloses or fairly suggests the feature of transposing an output of a final round from the plurality of transformation rounds, as recited by each of the amended independent claims. Further, as discussed in the present application at page 9, lines 23-27, this claim feature enhances the compatibility of the claimed invention.

Accordingly, it is submitted that amended independent Claims 21, 31, and 48 are patentable over the prior art. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

In re Patent Application of
MACCHETTI ET AL.
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**
_____________________________/

CONCLUSIONS

In view of the amendments to the claims and the arguments presented above, it is submitted that all of the claims are patentable. Accordingly, a Notice of Allowance is respectfully requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned at the telephone number listed below.

Respectfully submitted,

JACK GEORGE ABID
Reg. No. 58,237
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Applicants